DETAILED ACTION

Claims 2-25 Cancelled.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1, 26-38 are rejected under 35 U.S.C 103(a) as being unpatentable over Carolan et al (US Pat 7058022), in view of Epstein (US Pub 2002/0124064) in further view of Fukuda (US Pub 2003/0012156).

Consider Claim 1, Carolan disclosed the an information processing system comprising: a first information processing apparatus operable to authenticate a device (Carolan, Fig 1, Col 9 Lines 60-65, Carolan discloses RADIUS server, which can authenticate devices on the network); a second information

processing apparatus operable to hold setting information required to connect the device to a network (Carolan, Fig 1, Col 9 Lines 23-25, Carolan discloses the second information processing apparatus which at the service provider as a service activation system, which can for example hold a DHCP server, and DHCP server can contain hold setting information which is required for a device to connect to the network); and a third information processing apparatus connected to the network based on the setting information (Carolan, Fig 1, Col 5 Lines 43-62, Caroland discloses a client device which is enabled to be connected to the network, as its a network device, it can hold setting information obtained by a DHCP server, or it can also act a routing device etc); the first information processing apparatus including: a first storage unit operable to store first identification information for authenticating the third information processing apparatus (Carolan, Fig 1, Col 9 Lines 60-65, Carolan discloses RADIUS server, which can authenticate devices on the network), and second identification information for identifying the third information processing apparatus (Carolan, Fig 1, Col 9 Lines 23-25, Carolan discloses the second information processing apparatus which at the service provider as a service activation system, which can for example hold a DHCP server, and DHCP server can contain hold setting information which is required for a device to connect to the network, Col 7 Lines 50-53, Carolan also discloses on how the identity of the network client device is identified by its MAC address); an authenticating unit operable to authenticate the third information processing apparatus based on the first identification information in response to a request from the third information processing apparatus device (Carolan, Col 10, Lines 56-66, Carolan discloses on how the

authenticating unit such as registration server which can be a RADIUS server 'Fig 1, 162', authenticates the a request from the network client); a generating unit operable to generate third identification information that is used to connect the third information processing apparatus to the second information processing apparatus (Carolan, Col 10, Lines 56-66, Carolan discloses on how the network client device generates and transmits identification information such as MAC address, and subscriber's credentials to the service activation system 'Fig 1, 160' or the service provider network for processing); a second storage unit operable to store the third identification information in association with the second identification information (Carolan, Fig 1, Col 10 Lines 67, Col 11 Lines 1-15, Carolan discloses on how the service provider/service activation system maintains the information received from the network client device. The data is sent from and network client device and stored in the service provider/service activation system for processing, and if it is successful, the client can move on to perform other associated functions within the network. Further support can be seen in Col 11 Lines 50-57, Carolan discloses the use of a database to store the information); a first sending unit operable to send the third

identification information to the third information processing apparatus (Carolan, Fig 1, Col 9 Lines 60-65, Carolan discloses RADIUS server, which can authenticate devices on the network which is the third information processing apparatus); a first receiving unit operable to receive the third identification information from the second information processing unit (Carolan, Fig 1, Col 9 Lines 45-64, Carolan discloses on how the RADIUS system processing the identification system obtained from the service

provider/service activation system, Carolan discloses on how the DHCP/registration server can pass information of the network client to the first unit such as RADIUS Server for client authentication, prior to sending hold setting information to the network client device) and a second sending unit operable to send the second identification information to the second information processing apparatus (Carolan, Fig 1, Col 9 Lines 23-25, Carolan discloses the second information processing apparatus which at the service provider as a service activation system, which can for example hold a DHCP server, and DHCP server can contain hold setting information which is required for a device to connect to the network); the second information processing apparatus including: a third storage unit operable to store the setting information for connecting the third information processing apparatus to the network in association with the second identification information (Carolan, Fig 1, Col 10 Lines 67, Col 11 Lines 1-15, Carolan discloses on how the service provider/service activation system maintains the information received from the network client device. The data is sent from and network client device and stored in the service provider/service activation system for processing, and if it is successful, the setting information is sent to the client and then the client can move on to perform other associated functions within the network. Further support can be seen in Col 11 Lines 50-57, Carolan discloses the use of a database to store the information); a second receiving unit operable to receive the third identification information from the third information processing apparatus (Carolan, Col 10, Lines 56-66, Carolan discloses on how the network client device generates and transmits identification information such as MAC address, and subscriber's credentials to the

service activation system 'Fig 1, 160' or the service provider network for processing); a third sending unit operable to send the received third identification information to the first information processing apparatus (Carolan, Col 10, Lines 56-66, Carolan discloses on how the authenticating unit such as registration server which can be a RADIUS server 'Fig 1, 162', authenticates the a request from the network client); a third receiving unit operable to receive the second identification information from the first information processing apparatus (Carolan, Col 7 Lines 50-53, Carolan also discloses on how the identity of the network client device is identified by its MAC address); and a fourth sending unit operable to send the setting information stored in association with the received second identification information to the third information processing apparatus (Carolan, Fig 1, Col 10 Lines 67, Col 11 Lines 1-15, Carolan discloses on how the service provider/service activation system maintains the information received from the network client device. The data is sent from and network client device and stored in the service provider/service activation system for processing, and if it is successful, the setting information is sent to the client and then the client can move on to perform other associated functions within the network. Further support can be seen in Col 11 Lines 50-57, Carolan discloses the use of a database to store the information); and the third information processing apparatus including: a fourth storage unit operable to store the first identification information (Carolan, Col 5 Lines 45-50, Carolan discloses that the client device can have storage capabilities, and client does contain information related to its identification in Col 8 Lines 24-30); a requesting unit operable to request the first information processing apparatus to authenticate the third information processing

apparatus based on the first identification information stored in the fourth storage unit (Carolan, Fig 1, Col 9 Lines 45-64, Carolan discloses on how the RADIUS system processing the identification system obtained from the service provider/service activation system, Carolan discloses on how the DHCP/registration server can pass information of the network client to the first unit such as RADIUS Server for client authentication, prior to sending hold setting information to the network client device); a fourth receiving unit operable to receive the third identification information from the first information processing apparatus (Carolan, Fig 1, Col 9 Lines 45-64, the RADIUS server can obtain information from the client device, when the client is sending information regrading its authentication); a fifth sending unit operable to send the received third identification information to the second information processing apparatus (Carolan, Col 10, Lines 56-66, Carolan discloses on how the network client device generates and transmits identification information such as MAC address, and subscriber's credentials to the service activation system 'Fig 1, 160' or the service provider network for processing); and a fifth receiving unit operable to receive the setting information from the second information processing apparatus (Carolan, Fig 1, Col 9 Lines 23-25, Carolan discloses the second information processing apparatus which at the service provider as a service activation system, which can for example hold a DHCP server, and DHCP server can contain hold setting information which is required for a device to connect to the network).

Carolan does not explicitly disclose upon acquiring the first identification information including the device ID and the pass phrase, the first information processing

apparatus determines the second identification information including a product code and the serial number. Furthermore, Carolan does not explicitly disclose the third identification information including a one-time ID.

Nonetheless, Epstein discloses acquiring the first identification information including the device ID (Epstein, [0126], Epstein discloses on how the device ID and device profile are sent to the controller for processing) and the pass phrase (Epstein, [0062], Epstein discloses on how the pass phrase is used and generated by the system for authentication purposes), the first information processing apparatus determines the second identification information including a product code and the serial number (Epstein, [0117], [0125]-[0126], Epstein discloses on how the product code and serial number – device ID - from the devices is audited and identified). And Epstein discloses the third identification information including a one-time ID (Epstein, [0071], [0075], Epstein discloses on how one-time password is used to establish the underlying secure connection during the authentication process).

Both Carolan-Epstein provide features related to provide a secure management of processing system environment. Therefore one of ordinary skill in the art would have been motivated to combine the teachings since both are within the same environment.

Therefore, it would be obvious to a person skilled in the art to incorporate the use of ID, pass-phrase, product code and serial number, along with one-time ID taught Epstein, in the system of Carolan for enabling multi-tier security mechanisms to prevent unauthorized access to the networks.

But Carolan-Epstein does not explicitly disclose wherein the setting information includes an Internet service provider connection ID and a password.

Nonetheless, Fukuda discloses on the setting information which includes an Internet service provider connection ID and password (Fukuda, [0023], Fukuda discloses the use of Internet service provider ID and its password for connection purposes).

Both Carolan-Epstein-Fukuda provide features related to management of processing systems. Therefore one of ordinary skill in the art would have been motivated to combine the teachings since both are within the same environment.

Therefore, it would be obvious to a person skilled in the art to incorporate the storing of network setting information, taught by Fukuda to Carolan-Epstein's system for creating connection to the ISP.

Consider Claims 26-28, they have similar limitations, as they contain identical elements as recited in Claim 1. They are rejected under the same rational as to claim 1.

Consider Claim 29,–Carolan-Epstein-Fukuda discloses the information processing system of claim 1, wherein the first information processing apparatus is a device authentication server (Carolan, Fig 1, Col 9 Lines 60-65, Carolan discloses RADIUS server, which can authenticate devices on the network).

Consider Claim 30, Carolan-Epstein-Fukuda discloses the information processing system of claim 1, wherein the second information processing apparatus is an ISP download server (Carolan, Fig 1, Col 9 Lines 23-25, Carolan discloses the second information processing apparatus which at the service provider as a service activation system, which can for example hold a DHCP server, and DHCP server can contain hold setting information which is required for a device to connect to the network).

Consider Claim 31, Carolan-Epstein-Fukuda discloses the information processing system of claim 1, wherein the third information processing apparatus is a router (Carolan, Fig 1, Col 5 Lines 43-62, Caroland discloses a client device which is enabled to be connected to the network, as its a network device, it can hold setting information obtained by a DHCP server, or it can also act a routing device etc).

Consider Claim 32, Carolan-Epstein-Fukuda discloses the information processing system of claim 1, wherein the setting information includes an Internet service provider connection ID and a password (Fukuda, [0023], Fukuda discloses the use of Internet service provider ID and its password for connection purposes).

Consider Claim 33, Carolan-Epstein-Fukuda discloses the information processing system of claim 1, wherein the one-time ID is generated as a result of authentication of the device (Epstein, [0071], [0075], Epstein discloses on how one-time password is used to establish the underlying secure connection during the authentication process).

Consider Claim 34, Carolan-Epstein-Fukuda discloses the information processing system of claim 33, wherein the one-time ID contains no information relating to the third information processing apparatus or the first information processing apparatus (Epstein, [0071], [0075], Epstein discloses on how one-time password is used to establish the underlying secure connection during the authentication process and since it is only for connection purposes only).

Consider Claim 35, Carolan-Epstein-Fukuda discloses the information processing system of claim 1, wherein the first information processing apparatus determines the product code and the serial number based on a product registration number received (Epstein, [0117], [0125]-[0126], Epstein discloses on how the product code and serial number – device ID - from the devices is audited and identified).

Consider Claim 36, Carolan-Epstein-Fukuda disclose the information processing apparatus of claim 26, wherein the setting information includes an Internet service provider connection ID and a password (Fukuda, [0023], Fukuda discloses the use of Internet service provider ID and its password for connection purposes).

Consider Claim 37, Carolan-Epstein-Fukuda disclose the information processing apparatus of claim 27, wherein the setting information includes an Internet service provider connection ID and a password (Fukuda, [0023], Fukuda discloses the use of Internet service provider ID and its password for connection purposes).

Consider Claim 38, Carolan-Epstein-Fukuda disclose the device of claim 28, wherein the setting information includes an Internet service provider connection ID and a password (Fukuda, [0023], Fukuda discloses the use of Internet service provider ID and its password for connection purposes).

Response to Arguments

Applicant's arguments with respect to claims 1, 26-38 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANISH SIKRI whose telephone number is 571-270-1783. The examiner can normally be reached on 8am - 5pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia Dollinger can be reached on 571-272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Anish Sikri
a.s.

6/4/10

/Tonia LM Dollinger/

Supervisory Patent Examiner, Art Unit 2443